Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 14 July 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Trucker reports that trucking companies planning to haul certain highly hazardous materials must have a special safety permit beginning January 1, 2005. (See item 10)

- The Detroit Free Press reports a high−tech network of surveillance cameras is still not installed along Michigan's border with Canada and at other locations along the northern border. (See item 11)

- Microsoft has released "Security Bulletin MS04−022: Vulnerability in Task Scheduler Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item 28)

- Microsoft has released "Security Bulletin MS04−023: Vulnerability in HTML Help Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item 29)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical Industry and Hazardous Materials**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information Technology and Telecommunications**; **Internet Alert Dashboard**

Other: **Commercial Facilities/Real Estate, Monument &Icons**; **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 13, Associated Press* — **IEA foresees slowdown in world oil demand. Growth in world oil demand will slow to 2.2 percent in 2005, as China and other oil−hungry developing countries bump up against their limits for refining and transporting crude, the**

International Energy Agency (IEA) said Tuesday, July 13. Demand next year will average 83.2 million barrels a day, and crude supplies from Russia, Angola and Brazil will meet the bulk of the increased needs, the agency said in its monthly oil market report. The Paris−based IEA is the energy watchdog for wealthy oil−importing countries. It analyzes the supply and demand for crude, but avoids predicting prices. For 2004, the agency predicted that oil demand will surge by 3.2 percent to an average of 81.4 million barrels a day, due partly to the transfer of manufacturing activity to less energy−efficient developing nations and to rising consumption there. The IEA noted that global supplies rose in June by one percent, or 790,000 barrels a day, with the Organization of Petroleum Exporting Countries (OPEC) accounting for 635,000 barrels of the increase. **Although industrialized countries' inventories of crude rose to more comfortable levels in May, inventories of gasoline and other refined products remained tight, it said.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A46000−2004Jul 13.html

2. *July 13, Itar−Tass* — **Russia not to raise oil prices.** Unlike members of the Organization of Petroleum Exporting Countries (OPEC), Russia is not going to raise the price of oil, Valery Yazev, the chairman of the Energy, Transport and Communications Committee of the State Duma lower house of Russian parliament, said on Tuesday, July 13. **"Russia will respond to price rises at the leading oil markets by raising the export duty on oil," he said. Yazev believes the present situation in the world markets is favorable for Russia.** "The high demand for oil is the guarantee of the growth of Russia's export, and hence, of currency receipts," he said. "The situation suggests the lowering of deliveries, but Russia will be increasing exports in the foreseeable future."
   Source: http://www.itar−tass.com/eng/level2.html?NewsID=1034284&Page Num=0

3. *July 13, Associated Press* — **Parts of Tallahassee left in the dark.** Power was knocked out Tuesday, July 13, to about half of Tallahassee, FL, when generators serving the city failed. Officials said temperatures in the mid−90s likely played a part in the outage. **The brownout left about half the city's 97,000 power customers without electricity for a couple hours early Tuesday afternoon after the city's two main generating plants both failed around the same time,** said city spokesperson Bill Behenna. He said the city−owned utility was "on its way to a record load," when the generators failed, with temperatures in the mid−90s and a heat index around 100. Behenna said officials weren't sure yet whether high usage was definitely to blame, but expected it at least played a role in the power failure.
   Source: http://www.gainesvillesun.com/apps/pbcs.dll/article?AID=/200
   40713/APN/407130841

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 13, The Tribune−Review (PA)* — **Chemicals seized from Hempfield home. Authorities have seized an undisclosed amount of materials and chemicals that can be used to make explosive devices from a Hempfield Township, PA, home, state police at Greensburg reported Monday, July 12.** The Westmoreland County Hazmat Team and Allegheny County Bomb Squad responded to the residence, which sits on a hill overlooking Route 119. Police said they had a suspect. The case began as a complaint of a possible fireworks violation, according

to police. Authorities did not describe the type of substances found at the home. The Bureau of Alcohol, Tobacco and Firearms, Westmoreland County Sheriff's Department Special Services K−9 Unit, Westmoreland County Department of Public Safety and Hannastown Volunteer Fire Department also responded to the scene.
Source: http://pittsburghlive.com/x/tribune−review/trib/westmoreland /s_203138.html

5. *July 13, News 9 San Antonio (TX)* — **Office evacuated after sulfuric acid spill. A chemical spill prompted the evacuation of more than 20 employees from the TETCO office building in Northeast San Antonio, TX, Monday, July 12. The San Antonio Fire Department (SAFD) said a worker spilled sulfuric acid in the basement of the building.** Officials said the man received some burns and was taken to the hospital by his supervisor. The first floor of the building was evacuated after some people experienced breathing problems. One TETCO employee was taken to the hospital as a precaution. Others were treated with oxygen at the scene, while Hazmat crews cleaned up the spill. "What they did is absorb the spill with some pads and diluted the rest of it down that they couldn't pick up. Then they went around and took readings throughout the rest of the building to verify that the readings were so insignificant, that they would not pose harm to anyone else," SAFD Fire Chief Randy Jenkins said. All of the evacuated employees were allowed back in after the spill was cleaned up.
Source: http://news9sanantonio.com/content/top_stories/default.asp?A rID=13686

[Return to top]

Defense Industrial Base Sector

6. *July 13, Reuters* — **UK military: iPod is security risk.** Britain's Ministry of Defense (MoD) has become the latest organization to add the iPod to its list of high−tech security risks. **The pocket−sized digital music player, which can store thousands of songs, is one of a series of banned gadgets that the military will no longer allow into most sections of its headquarters in the United Kingdom and abroad.** Devices with large storage capabilities −− most notably those with a Universal Serial Bus (or USB) plug used to connect to a computer −− have been treated with greater suspicion of late by government agencies and corporations alike. **The fear is that the gadgets can be used to siphon information from a computer, turning a seemingly innocuous device into a handy tool for data thieves.** "With USB devices, if you plug it straight into the computer you can bypass passwords and get right on the system," said Royal Air Force Wing Commander Peter D'Ardenne. "That's why we had to plug that gap," he said, adding that the policy was put into effect when the MoD switched to the USB−friendly Microsoft XP operating system over the past year.
Source: http://www.cnn.com/2004/TECH/internet/07/13/britain.mod.reut /index.html

[Return to top]

Banking and Finance Sector

7. *July 13, Associated Press* — **Bank of America to buy bankcard processor. Bank of America said Tuesday, July 13, it is buying bankcard processor National Processing of Louisville, KY, in a $1.4 billion cash deal that would create the nation's second−largest such**

company with nearly $250 billion in annual processing volume. Under the terms of the agreement, Bank of America will pay $26.60 per share for the publicly held company, which will be merged with its Bank of America Merchant Services business. The newly combined business will be headquartered in Louisville. National Processing's merchant services business processes Visa and MasterCard transactions for some 700,000 merchants in North America. The company also provides financial settlement and reporting services to large and mid−size corporate customers in the travel and health care industries. The transaction is expected to be completed by the end of the year, subject to shareholder and regulatory approvals. Bank of America holds nearly $1 trillion in assets and has 35 million consumer and small business customers.
Source: http://www.nytimes.com/aponline/business/AP−Bank−of−America−National−Processing.html

8. *July 13, Reuters* — **Snow: terror threat hangs over economy.** The potential for more terror attacks is a risk to the U.S. economy that requires vigilance against any bid to weaken measures for investigating suspicious money transactions, U.S. Department of Treasury Secretary John Snow said on Tuesday, July 13. "Terrorism is a threat to the economy and it's awfully important that we keep our guard up and do all we can to keep the terrorists at bay," Snow said in a local radio interview. **Snow said terror groups cannot survive if their cash is choked off.** "Hatred fuels the terrorist agenda, cash makes it possible," he said in remarks prepared for delivery after a tour of a local film−coating plant later on Tuesday. **"The work to track and shut down the financial network of terror is, therefore, one of the most critical jobs of our government today."**
Source: http://www.nytimes.com/reuters/business/business−security−sn ow.html

9. *July 12, Washington Post* — **Senate bill targets phishers. Internet scam artists who use fake Websites to dupe people into revealing sensitive financial information could face up to five years in jail and forced to pay $250,000 in fines under a bill introduced recently in the Senate. The legislation, introduced Friday, July 9, is designed to fight "phishing,"** one of the newest and most dangerous forms of online fraud. Phishing threatens the integrity of secure shopping on the Internet and could hurt electronic commerce, said the bill's sponsor, Senator Patrick Leahy. Phishing scammers already violate a host of identity theft and fraud laws, but prosecuting them under those statutes can be challenging, said Rich Phillips, a Leahy aide. To charge scammers now, law enforcers need to prove that a victim suffered measurable losses. By the time they do that, he said, the scammer has often disappeared. Phishing victims lost $1.2 billion to identity theft−related fraud between April 2003 and April 2004, and were three times more likely than the average American to have their identities stolen, according to an online survey of 5,000 people conducted in May by Stamford, CT−based firm Gartner Research.
Source: http://www.washingtonpost.com/wp−dyn/articles/A44826−2004Jul 12.html

[Return to top]

Transportation Sector

10. *July 14, The Trucker* — **Some hazmat carriers must have safety permit in 2005.** Trucking companies planning to haul certain highly hazardous materials must have a special safety permit beginning January 1, 2005, the Federal Motor Carrier Safety Administration (FMCSA)

announced Wednesday, June 30. The permit is required, according to the FMCSA, because certain highly hazardous materials would be more dangerous in crashes or if used in terrorist attacks. **The safety permit will be required for motor carriers hauling certain types and amounts of radioactive materials, explosives, toxic inhalant materials and compressed or refrigerated liquid methane or natural gas**. According to FMCSA estimates, the annual safety benefits to the U.S. economy resulting from fewer accidental releases of hazardous materials will be $3.7 million, which over a 10−year period will result in safety benefits totaling more than $26 million after adjustment for inflation.
Source: http://www.thetrucker.com/stories/07_04/0712_safety_permit.h tml

11. *July 13, Detroit Free Press* — **Surveillance system lacking at U.S.−Canada border. A year after officials expected the system to be up and running, a much−hailed high−tech network of surveillance cameras is still not installed along Michigan's border with Canada and at other locations along the northern border.** The Detroit sector of the U.S. Border Patrol monitors 804 miles of border with Canada. The region was originally slated to get eight cameras, called remote video surveillance, last year. But now it is unclear when the system will arrive. Robert Bonner, commissioner for U.S. Customs and Border Protection, told a congressional panel in October that 238 remote video surveillance sites were completed and operating along the United States' northern and southern borders. Sixty−eight were installed on the northern border, he said, and an additional 224 installations are proceeding nationwide. **Border agents have said the cameras are an important tool for an agency that is strapped for manpower and is supposed to be guarding against terrorists, drug runners and human smuggling.** Though there have been reported reliability problems with the system, in border cities like Blaine, WA, where 32 cameras are installed, drug seizures and arrests of illegal immigrants have increased, according to government records.
Source: http://www.tallahassee.com/mld/tallahassee/news/nation/91426 83.htm

12. *July 13, Atlanta Business Chronicle* — **Hartsfield−Jackson begins TSA baggage screening project.** Hartsfield−Jackson Atlanta International Airport in Atlanta, GA, will begin building the Transportation Security Administration's (TSA) in−line baggage screening facilities near the North and South Terminals on Friday, July 16 and Wednesday, July 21, respectively. **A special government−airport partnership will make the federally mandated project a reality at an estimated cost of $215 million. Once complete, the TSA Baggage Screening Project will help ensure a more efficient baggage check−in process for travelers**. Constructed in two phases, the two underground facilities will accommodate the electronic security screening of checked baggage. Airport representatives expect to have both phases of the construction completed within 12 to 15 months from the initial start dates.
Source: http://atlanta.bizjournals.com/atlanta/stories/2004/07/12/da ily10.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *July 13, USAgNet* — **Guidelines to poultry industry to prevent flu.** Avian influenza is a highly contagious disease of birds, which is currently epidemic in Asia. **U.S. Occupational Safety and Health Administration (OSHA) issued guidelines to protect farm, processing plant, and food distribution workers from exposures to avian influenza virus. These guidelines reduce the likelihood of illness or gene swapping or mutation.** The guidelines include recommendations on hand hygiene. Additionally, all workers involved in the culling, transport, or disposal of avian influenza−infected poultry should be provided with appropriate personal protective equipment including an impermeable apron or surgical gowns with long cuffed sleeves, an impermeable apron, gloves capable of being disinfected or disposed, eye goggles, and respirators. Unvaccinated workers should receive the current season's influenza vaccine to reduce the possibility of dual infection with avian and human influenza viruses. Workers should, also, receive an influenza antiviral drug daily for the duration of time during which direct contact with infected poultry or contaminated surfaces occurs.
Source: http://www.usagnet.com/story−national.cfm?Id=724&yr=2004

14. *July 12, Animal and Plant Health Inspection Service* — **Chile recognized as free of classical swine fever.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service Monday, July 12, announced that it is amending its regulations by adding Chile to the list of regions considered free of classical swine fever (CSF). Chile also is added to a list of CSF−free regions that must meet certain certification requirements. **This amendment will allow Chile to export live swine, swine semen, pork, and pork products to the United States.** The certification requirements for origin and handling are intended to ensure that exports of these commodities do not pose a risk of introducing CSF into the United States. Classical swine fever, also known as hog cholera, is a highly contagious viral disease of swine found throughout the world. The U.S. has been free of the disease since 1976. This final rule is scheduled for publication in the Tuesday, July 13 Federal Register and becomes effective July 28.
Source: http://www.aphis.usda.gov/lpa/news/2004/07/csfchile_vs.html

15. *July 12, High Plains Journal (KS)* — **Be alert for rust, APHIS says. U.S. soybean growers should be educating themselves about Asian soybean rust and sharpening their field−scouting skills this season, Animal Plant Health Inspection Service (APHIS) and industry leaders said Friday, July 9.** During a teleconference with farm reporters, officials outlined the response plan if Asian soybean rust enters the U.S. and addressed the question of what will happen this year or down the road. "We all need to get a lot smarter on what it (soybean rust) is and how we can react when it gets here," said David Durham, United Soybean Board communications chairman. "It's vital that farmers hear accurate information and producers need to know it's a manageable disease. They (farmers) need to know they can go to a crop consultant to react quickly to this fungus." The devastating fungus has not been detected in the United States. U.S. Department of Agriculture officials reported they have confidence the Environmental Protection Agency (EPA) would be approving all requested fungicides for use for Section−18 emergency purposes.
Source: http://www.hpj.com/dtnnewstable.cfm?type=story&sid=12156

[Return to top]

Food Sector

16. *July 13, American City Business Journals* — **Trail mix bars recalled. Milwaukee, WI, based Pick 'n Save grocery store operator Roundy's Inc. is recalling a fruit and nut bar because it contains almonds that may have been contaminated with salmonella.** The recall covers 7.4−ounce boxes of Roundy's Chewy Trail Mix Bars, Fruit & Nut. The units were sold in Pick 'n Save stores and other stores serviced by Roundy's primarily in Wisconsin and Ohio. The product recall is in response to a voluntary recall by Paramount Farms of California of whole and diced raw almonds, based on more than 20 reports of possible illnesses nationwide, Roundy's said.
Source: http://milwaukee.bizjournals.com/milwaukee/stories/2004/07/1 2/daily15.html

17. *July 13, WRTV (IN)* — **Vaccine could protect against food poisoning.** An Ohio scientist says he has concocted a vaccine that someday could protect people from food poisoning caused by bacteria. John Gunn, a scientist with the Ohio State University Medical Center, said lab tests have shown a dose can offer six months of protection. **"We've been able to show in a single oral dose, 100 percent protection against both salmonella and listeria," Gunn said.** Researchers hope to develop doses that offer years of protection.
Source: http://www.theindychannel.com/health/3513957/detail.html

[Return to top]

Water Sector

18. *July 13, NBC5 (IL)* — **Water main break causes problems. About 70,000 people in Kankakee, IL, were affected by a water main break there, and a boil order remained in effect Tuesday, July 13.** The water is back on now, but it is unsafe to use, NBC5's Charlie Wojciechowski reported. The pipe that broke was 80 years old and carried about 12,000 gallons of water. **The break left the Kankakee, Bradley, and Bourbonnais area without useable water on Monday, July 12.** Many residents and businesses didn't have water coming out of their taps at all. The taps are working again, but a boil order is in effect for the three communities. The break was so severe because the pipe that broke was the one directly in front of the pumping station −− the only way to get water in and out of that station.
Source: http://www.nbc5.com/news/3521129/detail.html?z=dp&dpswid=226 5994&dppid=65194

[Return to top]

Public Health Sector

19. *July 13, Cape Cod Times (MA)* — **Tularemia probable on Vineyard again.** It is high on the government's list of potential bioterrorism agents, but you're far more likely to encounter tularemia while mowing a lawn. **The confirmation by Massachusetts health officials this week of a Tisbury landscaper's "probable case" of tularemia, or "rabbit fever," means that the potentially deadly bacterial disease has struck on Martha's Vineyard for the fifth**

straight summer. The persistence of the illness on the island has scientists baffled and has locals on alert. Tularemia can be contracted either through a bite by an infected dog tick, by inhaling the highly infectious spores from an infected animal, or through contact with the bacteria through an open cut or sore. The version of the illness transmitted through a tick bite or through an open sore creates a lesion on the skin and can also lead to swollen lymph nodes and flu−like symptoms. The inhaled version, which is the bioterrorism concern, causes a pneumonia−like condition, which is more dangerous than the skin version. Untreated, about seven percent of victims die. Prior to 2000, Martha's Vineyard had not had an outbreak since 1978, when 12 people were stricken.
Source: http://www.capecodonline.com/cctimes/tularemiaxz13.htm

20. *July 13, Howard Hughes Medical Institute* — **Steps needed to lessen smallpox threat. The best approach for averting the deadly spread of smallpox following release of the virus by terrorists may rest with the establishment of a major collaborative research effort to develop new antiviral drugs that would involve the pharmaceutical and biotechnology industries, universities, and government agencies, according to the National Academies.** According to Howard Hughes Medical Institute investigator Stephen C. Harrison, two factors loomed large as the scientists considered the dangers of smallpox. First, there is essentially no information about whether stocks of the variola virus, which causes smallpox, exist outside the two known repositories in the U.S. and Russia. Second, the impact of intentional release of the virus would "probably provoke a global health crisis." Given the pressing need for novel drugs to prevent the spread of smallpox if it were to be used as a bioterror agent, Harrison said that the group's top recommendation was the immediate engagement of biotechnology and pharmaceutical companies in the project. Antiviral drugs against smallpox are needed because vaccines produce substantial side effects. **The development of antiviral drugs against smallpox could deter rogue states or terrorists from releasing the virus because its impact would be diminished.**
Source: http://www.innovations−report.com/html/reports/life_sciences /report−31168.html

21. *July 13, Medical News Today* — **National Bioinformatics Resource Center to support infectious disease research.** The Virginia Bioinformatics Institute (VBI) and its partners have been awarded a five−year, $10.3 million contract from the National Institute of Allergy and Infectious Diseases (NIAID). **The purpose of this contract is to establish a national Bioinformatics Resource Center (BRC) that consists of a multi−organism relational database in support of infectious disease research, especially as it affects biodefense and emerging infectious diseases.** VBI's BRC will focus on Brucella (causes Brucellosis in cattle, pigs, and humans), Caliciviruses (causes many of the viral dysenteries on cruise ships), hepatitis A, Rabiesvirus, Coxiella burnetii/Rickettsias (which cause Q fever, Rocky Mountain spotted fever, and typhus). "The BRC will allow researchers throughout the world to access, analyze, and study molecular data for these infectious diseases as interoperable components to support biological synthesis," said VBI professor Bruno Sobral. Researchers will be able to store, view, display, query, annotate, and analyze genomic and related data and bibliographic information.
Source: http://www.medicalnewstoday.com/medicalnews.php?newsid=10638

22. *July 13, Associated Press* — **Whooping cough makes a comeback .** Whooping cough, one of those ancient scourges that infant vaccination was meant to wipe out, is making a dangerous

comeback: it turns out the vaccine that babies get starts wearing off by adolescence. **With outbreaks striking teenagers and adults, the government soon will decide if it's time for booster shots against the whooping cough.** Whooping cough can kill newborns before they start getting their vaccinations. And while older patients usually recover, they can easily spread the disease, known medically as pertussis, to infants. The incidence of pertussis plummeted in industrialized nations after vaccination began in the 1940s. It now is on the rise again globally. Why isn't clear, but it's thought to be at least partly due to waning immunity. Children get five doses of pertussis vaccine between ages two months and six years. The protection begins to drop five to 10 years after the last shot. **In the U.S., a preliminary Center for Disease Control and Prevention count found more than 11,000 pertussis cases last year. That's up from 9,771 the previous year. Experts say there may be 10 times as many cases, even more.** Studies suggest almost a quarter of people with coughs that last longer than two weeks have undiagnosed pertussis, said Kathryn Edwards of Vanderbilt University.
Source: http://www.zwire.com/site/news.cfm?newsid=12317623&BRD=1710&PAG=461&dept_id=377222&rfi=6

23. *July 12, National Public Radio* — **Plague outbreaks help scientists hone method for tracing attacks.** In a typical year, several people in the U.S. come down with an unusual disease: the plague. It's often transmitted by fleas that carry it from prairie dogs or other rodents. But there's another possible source of plague infection −− bioterrorist attacks. The plague ranks high on the list of biological weapons that might be used in a terrorist attack; a single bacterium in the lungs can trigger the disease. **So scientists are searching for a way to quickly determine if a case is natural or criminal. For answers, they're turning to prairie dogs living outside Flagstaff, AZ.** It's not unusual for an outbreak to kill an entire colony of wild prairie dogs. **A group of Northern Arizona University researchers collect plague−carrying fleas from the burrows and analyze the bacteria's DNA.** They then characterize the different strains and pinpoint the geographic regions where they're found.
Source: http://www.npr.org/features/feature.php?wfId=3343000

[Return to top]

Government Sector

24. *July 12, Federal Computer Week* — **Senators sponsor homeland security grant bill.** Two senators introduced bipartisan legislation recently to establish an intergovernmental grant program to develop or modify homeland security equipment, technologies, capabilities and services. **The bill (S. 2635), introduced by Senator Susan Collins and Senator Joseph Lieberman, would require Department of Homeland Security officials to conduct a needs assessment of federal, state and local governments and then survey existing products or services within the United States or other countries focused on homeland security.** Grants would fund joint ventures among businesses, academic institutions, or nonprofit groups, and other entities that have demonstrated counterterrorism or homeland security capabilities. The bill authorizes $25 million for fiscal 2005. "This program will act as a revolving fund to develop new homeland security technologies," Collins said. "As these technologies are deployed and become profitable, the businesses that developed them will be required to repay the program for the amount of the funds. This requirement, which has worked for similar existing programs, will help sustain the availability of funds for future funds."

Source: http://www.fcw.com/fcw/articles/2004/0712/web−bills−07−12−04 .asp

25. *June 25, Government Accountability Office* — **GAO−04−682: Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System (Report).** Established in March 2002, **the Homeland Security Advisory System was designed to disseminate information on the risk of terrorist acts to federal agencies, states, localities, and the public. However, these entities have raised questions about the threat information they receive from the Department of Homeland Security (DHS) and the costs they incurred as a result of responding to heightened alerts.** This report examines (1) the decision making process for changing the advisory system national threat level; (2) information sharing with federal agencies, states, and localities, including the applicability of risk communication principles; (3) protective measures federal agencies, states, and localities implemented during high (code orange) alert periods; (4) costs federal agencies reported for those periods; and (5) state and local cost information collected by DHS.
Highlights: http://www.gao.gov/highlights/d04682high.pdf.
Source: http://www.gao.gov/new.items/d04682.pdf

[Return to top]

Emergency Services Sector

26. *July 13, Associated Press* — **Consultants fault lack of planning in fire response. An analysis of Rhode Island's emergency response to a nightclub fire that killed 100 people by Titan Corp. found significant problems in the state's readiness for a disaster, particularly with its capacity for communication between agencies and for marshaling resources.** The report funded by the Department of Homeland Security concluded that the first responders were not supported, and in some cases were hampered, by the lack of a comprehensive statewide plan for disaster response. In its evaluation, Titan said while the state Emergency Management Agency might have been expected to play the lead role in coordinating a response, the state never implemented its "Mass Casualty Disaster" plan or activated the state Emergency Operations Center. The lack of planning for such a disaster was so extreme, the report said, that faced with an overwhelming number of victims and needing to summon more ambulances, Warwick Fire Battalion Chief Henry Heroux instructed his city's fire alarm office "to use the Yellow Pages and ask private ambulance companies to respond with as many ambulances as possible."
Source: http://www.boston.com/dailynews/195/region/Consultants_fault_ lack_of_plan:.shtml

[Return to top]

Information Technology and Telecommunications Sector

27. *July 13, Associated Press* — **Man indicted for allegedly infiltrating phone system.** A Westchester, NY, man has been indicted on charges he penetrated a central computer that Verizon uses in repairing telephone lines. William Quinn engaged in a practice called "phreaking" −− breaking into the phone system −− more than 100 times this year, according to the indictment filed Monday, July 12, in Manhattan federal court. Many "phreakers" try to infiltrate phone company computers to steal phone service. Quinn posted the passwords and

directions on how to use them on several Websites, the indictment alleged. **Prosecutors said they were taking a tough approach to telephone security violations because of the risk that a hacker could cripple the system during an emergency.** They alleged that Quinn broke into a computer that can turn service on and off on all Verizon phone lines. "In so doing, Quinn acquired the same ability as an authorized Verizon employee to test and disable telephone numbers within various telephone area codes across the country," according to the indictment.
Source: http://www.usatoday.com/tech/news/computersecurity/2004−07−13−phreaking−indictment_x.htm

28. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−022: Vulnerability in Task Scheduler Could Allow Code Execution.** A remote code execution vulnerability exists in the Task Scheduler because of an unchecked buffer. **If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system**, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. However, user interaction is required to exploit this vulnerability. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−022. mspx

29. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−023: Vulnerability in HTML Help Could Allow Code Execution.** This update resolves two newly−discovered vulnerabilities. The HTML Help vulnerability was privately reported and the showHelp vulnerability is public. **If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system**, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−023. mspx

30. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−019 Vulnerability in Utility Manager Could Allow Code Execution.** A privilege elevation vulnerability exists in the way that Utility Manager launches applications. **A logged−on user could force Utility Manager to start an application with system privileges and could take complete control of the system.** An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−019. mspx

31. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−020: Vulnerability in POSIX Could Allow Code Execution.** A privilege elevation vulnerability exists in the POSIX operating system component (subsystem). **An attacker who successfully exploited this vulnerability could take complete control of an affected system**, including installing

programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the update immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−020. mspx

32. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−021: Security Update for IIS 4.0.** This update resolves a newly−discovered, privately reported vulnerability. **An attacker who successfully exploited this vulnerability could take complete control of an affected system**, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−021. mspx

33. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−024: Vulnerability in Windows Shell Could Allow Remote Code Execution.** A remote code execution vulnerability exists in the way that the Windows Shell launches applications. **If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system**, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. However, significant user interaction is required to exploit this vulnerability. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−024. mspx

34. *July 13, Microsoft* — **Microsoft Security Bulletin MS04−018: Cumulative Security Update for Outlook Express.** This update resolves a public vulnerability. **A denial of service vulnerability exists in Outlook Express because of a lack of robust verification for malformed e−mail headers**. This update also changes the default security settings for Outlook Express 5.5 Service Pack 2 (SP2). **If a user is running Outlook Express and receives a specially crafted e−mail message, Outlook Express would fail**. If the preview pane is enabled, the user would have to manually remove the message, and then restart Outlook Express to resume functionality. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−018. mspx

35. *July 12, US−CERT* — **Vulnerability Note VU#645326: MySQL fails to properly handle overly long "scramble" values.** MySQL is an open−source database system available for Microsoft Windows, Linux, and other UNIX−based operating systems. **There is a vulnerability in MySQL in which an overly long "scramble" string generated by the my_rnd() function could cause a buffer overflow to occur.** It has been reported that versions 4.1 prior to 4.1.3 and version 5.0 are affected. A remote, unauthenticated attacker could cause a denial of service or potentially execute code of the attacker's choice. According to the NGSSoftware Security Advisory, this vulnerability has been fixed in version 4.1.3 (Beta) and version 5.0 (Alpha): http://www.nextgenss.com/advisories/mysql−authbypass.txt
Source: http://www.kb.cert.org/vuls/id/645326

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Keylogger trojans such as Download.JECT, Scob and Berbew have garnered national attention by both the media and incident response teams. Microsoft has released an out−of−band fix for Internet Explorer to prevent future exploits of client machines using the ADODB vulnerability. See Microsoft's security bulletin here: http://www.microsoft.com/security/incident/download_ject.msp x

Current Port Attacks

Top 10 Target Ports	135 (epmap), 137 (netbios−ns), 9898 (dabber), 445 (microsoft−ds), 1434 (ms−sql−m), 5554 (sasser−ftp), 4899 (radmin), 139 (netbios−ssn), 3127 (mydoom), 1026 (nterm) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

36. *July 13, Journal News (NY)* — **Bomb threat forces Larkin Plaza evacuation. A state Department of Motor Vehicles (DMV) office, the Yonkers Riverfront Library and the city's Board of Education headquarters, all in Larkin Plaza in downtown Yonkers, NY, were evacuated Monday, July 12, after someone called the state agency threatening to blow it up, authorities said**. State and local authorities said a caller telephoned the DMV, which is near the Yonkers train station, around 1:15 p.m. and threatened to explode a bomb at 2:15 p.m. Yonkers police evacuated the three buildings, along with some other smaller ones nearby, and cordoned off Larkin Plaza with yellow police tape to keep civilians at a safe distance. Meanwhile, the Westchester County, NY, Department of Public Safety's (DPS) bomb squad was called in to search the DMV building, along with a K−9 unit from the Yonkers Emergency Service Unit. About 15 Yonkers firefighters stood by with fire engines. The bomb scare ended around 3:30 p.m., when law enforcement officials were satisfied there was no bomb in the building.
Source: http://www.thejournalnews.com/newsroom/071304/b0313evac.html

37. *July 13, Philadelphia Inquirer (PA)* — **Authorities seek man in photos to ask him about device. On Monday, July 12, the Philadelphia Joint Terrorism Task Force (JTTF) released photographs of a man wanted for questioning in connection with the Friday, July 9, discovery of an explosive device in shrubbery near the Philadelphia City Hall**. Police were called at 3:30 p.m. Friday by a person who told them about the device in the shrubs near

the southwest corner of Dilworth Plaza. Police found a black, hard plastic case similar to a tool box that contained a clear plastic tube filled with brownish−gray powder and blue paper at either end. Flame came from the package when the device was defused, police said. Authorities said they believed the same person phoned in bomb threats Saturday and Monday.
Source: http://www.philly.com/mld/inquirer/news/local/states/new_jer sey/9140879.htm?1c

[Return to top]

General Sector

38. *July 13, Reuters* — **Mine attack hits Chechen leader's convoy. A land mine blasted a convoy carrying Chechnya's pro−Moscow acting president on Tuesday, July 13, killing one person, though the president escaped injury, Russian news agencies said.** Itar−Tass news agency said the blast hit Sergei Abramov's convoy as it sped through Grozny, regional capital of the rebel Russian region. One member of his staff was killed, two were injured, but Abramov escaped unscathed, it said. Abramov took over as interim leader in the turbulent territory after its president Akhmad Kadyrov was killed by a bomb attack on May 9 during public celebrations. Elections for a new president are being held on August 29. An interior ministry official said the person who was killed was a bodyguard of Abramov.
Source: http://www.reuters.com/newsArticle.jhtml?type=worldNews&stor yID=5656452

39. *July 13, Bloomberg* — **Germany will expel terror suspects. Germany will expel Mounir el−Motassadeq and Abdelghani Mzoudi, both awaiting final decisions in court cases for alleged involvement in the September 11, 2001, terrorist attacks, once the final rulings have been handed down**, the Hamburg state Interior Ministry said. The ministry notified the two Moroccan nationals of its intent to expel them Monday, July 12, the ministry said in a statement. **El−Motassadeq, 30, was sentenced in February 2003 to 15 years in prison for involvement in the murder of more than 3,000 people and for being a member of the Hamburg terror cell that carried out the September 11 attacks. The ruling was overturned by the Federal Court of Justice March 4**. He is now awaiting his retrial, starting this summer. Mzoudi, 31, the second man to stand trial for the attacks, was acquitted in February 2004 because prosecutors failed to prove he helped plan the acts. The Federal Prosecutor's Office said at the time it would appeal the decision in the federal court. The authorities can only go ahead with el−Motassadeq's and Mzoudi's deportation after all the appeals in both court cases have been completed, the ministry said. The men will be able to appeal the order.
Source: http://quote.bloomberg.com/apps/news?pid=10000100&sid=axOkri 0FEmjM&refer=germany

40. *July 13, Associated Press* — **Oil tanker refuses to visit Basra due to terror threat. The crew of a Hong Kong−registered oil tanker the Venture Spirit refused to dock in the Iraqi oil terminal of Basra out of fears of terror attacks, the company that owns the ship said Tuesday, July 13. Chief Executive George Chao of Wah Kwong Shipping said he went along with the crew's decision because he was worried about the security situation in Iraq and a recent terror threat against several shipping companies.** He said he was concerned about the safety of his crew, the ship and the oil it was carrying, adding the ship was worth $100 million. Chao declined to say how much oil the tanker was scheduled to pick up or where

it was to have been delivered. The Venture Spirit has been under a five−year charter to Teekay Shipping, a crude oil shipper, since last June. Chao said it is now being replaced by another ship that will pick up the oil in Basra. The incident comes after South Korean intelligence officials said on Saturday, July 10, that Islamic militants posted an online message threatening attacks against ships carrying U.S. military goods in the Middle East.
Source: http://www.boston.com/dailynews/195/world/Hong_Kong_oil_tank er_refuses_t:.shtml

41. *July 13, Associated Press* — **Hundreds flee flooding in Northeast. A foot or more of rain fell in parts of the Northeast, forcing hundreds of people from their homes overnight Tuesday, July 13, rupturing small dams, and flooding roads.** No injuries had been reported in the stricken areas of New Jersey, Pennsylvania, and Maryland. South−central New Jersey was hardest hit with at least five small dams rupturing during the night, said Kevin Tuno, the Burlington County emergency management coordinator. Many of the dams in the area hold small reservoirs in low−lying residential areas. The heaviest rainfall in Burlington County was 13.2 inches at Tabernacle, the National Weather Service said. Governor James E. McGreevey said he plans to declare a state of emergency for the county. More than 500 county residents were evacuated from their homes and from the roofs of cars stalled on flooded roads. Parts of northeastern Maryland received up to eight inches of rain that flooded streets and basements, and some motorists had to be rescued when their cars stalled in deep water, officials said.
Source: http://www.mlive.com/newsflash/national/index.ssf?/base/national−27/108972204437180.xml

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.

Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.